Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Vragen gesteld door de leden der Kamer

2015Z09552

Vragen van het lid **Oosenbrug** (PvdA) aan de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *het gebruik van een softwarefout door de Amerikaanse inlichtingendiensten* (ingezonden 27 mei 2015).

Vraag 1
Heeft u kennisgenomen van het bericht «Het grootste deel van veilige internetverbindingen is kapot»?[1] Bent u op de hoogte van de berichtgeving over de «LogJam bug», die ervoor zorgt dat belangrijke versleutelingsprotocollen te omzeilen zijn?

Vraag 2
Heeft u kennisgenomen van het wetenschappelijk artikel, waarin aannemelijk wordt gemaakt dat de National Security Agency (NSA) de kwetsbaarheden in belangrijke versleutelingsprotocollen heeft gebruikt om beveiligde communicatie af te luisteren?[2]

Vraag 3
Onderschrijft u de waarneming van de wetenschappers dat gebruik van de nu onthulde kwetsbaarheden in versleutelingsprotocollen een zeer aannemelijke verklaring biedt voor de beveiligde informatie, waarvan afgelopen jaar duidelijk is geworden dat de NSA erover beschikt? Zo nee, waarom niet?

Vraag 4
Erkent u het belang van betrouwbare vormen van informatiebeveiliging voor een goed functionerende digitale samenleving? Hoe verhoudt zich dat tot het gebruik of zelfs het actief aanbrengen van kwetsbaarheden door overheden?

Vraag 5
Deelt u de mening dat overheden de veiligheid van de digitale samenleving ondermijnen door kwetsbaarheden niet te melden, maar te gebruiken om zich toegang tot informatie en systemen te verschaffen? Zo nee, waarom niet? Zo ja, hoe verhoudt dit gedrag zich tot internationale afspraken om de veiligheid van de digitale samenleving te vergroten?

---

[1] http://politiek.thepostonline.nl/2015/05/25/het-grootste-gedeelte-van-veilige-internetverbindingen-is-kapot/

[2] https://weakdh.org/imperfect-forward-secrecy.pdf

Vraag 6
Maken de Nederlandse inlichtingendiensten en de politie ook gebruik van onbekende kwetsbaarheden? Zo ja, hoe beoordeelt u de ondermijning van de veiligheid die door dit gebruik veroorzaakt wordt?

Vraag 7
Op welke wijze gaat de Nederlandse overheid om met al dan niet bewust aangebrachte kwetsbaarheden in software en hardware? Ondersteunt u de actieve opsporing van dergelijke kwetsbaarheden? Wordt er in aanbestedingen rekening gehouden met de mogelijke aanwezigheid van kwetsbaarheden? Worden kwetsbaarheden, die ontdekt worden, altijd gemeld zodat andere gebruikers zich hiertegen kunnen beveiligen?

Vraag 8
Hoe informeert het Nationaal Cyber Security Centrum (NCSC) bedrijven en burgers bij de ontdekking van ingrijpende kwetsbaarheden als bij deze «LogJam bug»? Welke mogelijkheden zijn er om de risico's van deze kwetsbaarheid te minimaliseren?

Vraag 9
Voert het NCSC of een andere partij onderzoek uit naar de mate waarin de Nederlandse digitale infrastructuur, in het bijzonder die van de overheid, getroffen is door deze kwetsbaarheid? Zo nee, wilt u hiertoe opdracht geven?